Quantum Communication Complexity Protocol with Two Entangled Qutrits

Časlav Brukner,[1] Marek Żukowski,[1,2] and Anton Zeilinger[1]
[1]Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090
[2]Instytut Fizyki Teoretycznej i Astrofizyki Uniwersytet Gdański, PL-80-952 Gdańsk, Poland
(Received 8 May 2002; revised manuscript received 16 August 2002; published 18 October 2002)

We formulate a two-party communication complexity problem and present its quantum solution that exploits the entanglement between two qutrits. We prove that for a broad class of protocols the entangled state can enhance the efficiency of solving the problem in the quantum protocol over any classical one *if and only if* the state violates Bell's inequality for two qutrits.

DOI: 10.1103/PhysRevLett.89.197901 PACS numbers: 03.67.Hk, 03.65.Ud, 42.50.Ar

Entanglement is not only the most distinctive feature of quantum physics with respect to the classical world, as quantitatively expressed by the violation of the Bell's inequalities [1]. It also enables powerful computation [2], establishes secure communication [2], and reduces the communication complexity [3–8], all beyond the limits that are achievable on the basis of laws of classical physics.

To date, only very few tasks in quantum communication and quantum computation require higher-dimensional systems than qubits as recourses. Quantum-key distribution based on higher alphabets was shown to be more secure than that based on qubits [9]. A certain quantum solution of the coin-flipping problem uses qutrits (three-dimensional quantum systems) [10], and the quantum solution of the Byzantine agreement problem utilizes the entanglement between three qutrits [11].

Here we formulate a two-party communication complexity problem and present its quantum solution which makes use of the entanglement between *two* qutrits. We prove that for a broad class of protocols the entangled state of two qutrits can enhance the efficiency of solving the problem in the quantum protocol, over any classical one *if and only if* the state violates Bell's inequality for two qutrits as derived by Collins *et al.* [12].

In this Letter, a variation of the following communication complexity problem will be considered. Two separated parties (Alice and Bob) receive some input data of which they know only their own data and not the data of the partner. Alice receives an input string x and Bob an input string y and the goal is for both of them to determine the value of a certain function $f(x, y)$, while exchanging a *restricted* amount of information. While an error in computing the function is allowed, the parties try to compute it correctly with as high a probability as possible. An execution is considered successful if the value determined by both parties is correct. Before they start the protocol, Alice and Bob are allowed to share (classically correlated) random strings which might improve the probability of success.

In 1997 Buhrman, Cleve, and van Dam [7] considered a specific two-party communication complexity problem of the type given above. Alice receives a string $x = (x_0, x_1)$ and Bob a string $y = (y_0, y_1)$. Each of the strings is a combination of two bit values: $x_0, y_0 \in \{0, 1\}$ and $x_1, y_1 \in \{-1, 1\}$. Their common goal is to compute the function (a reformulation of the original function of [7])

$$f(x, y) = x_1 y_1 (-1)^{x_0 y_0}, \quad (1)$$

with as high a probability as possible, while exchanging altogether only 2 bits of information. Buhrman *et al.* [7] showed that this can be done with a probability of success of $P_Q = 0.85$ if the two parties share two qubits in a maximally entangled state, whereas with shared random variables but without entanglement (i.e., in a classical protocol), this probability cannot exceed $P_C = 0.75$. Therefore, in a classical protocol 3 bits of information are *necessary* to compute f with a probability of at least 0.85, whereas with the use of entanglement 2 bits of information are *sufficient* to compute f with the same probability.

There is a link between tests of Bell's inequalities and quantum communication complexity protocols. Bell's inequalities are bounds on certain combinations of probabilities or correlation functions for measurements on multiparticle systems. These bounds apply for any local realistic theory. In a realistic theory the measurement results are determined by properties the particles carry. In a local theory the results obtained at one location are independent of any actions performed at spacelike separation. The quantum protocol of the two-party communication complexity problem introduced in Refs. [7,8] is based on a violation of the Clauser-Horne-Shimony-Holt [13] inequality. Similarly three- and multiparty communication complexity tasks were introduced [7,8,14] with quantum solutions based on the Greenberger-Horne-Zeilinger–type [15] argument against local realism.

Let us now define the two-party communication complexity problem which will be our case of study. This problem is of a different kind than the standard communication complexity problem where the two parties try to

 0031-9007/02/89(19)/197901(4)$20.00 © 2002 The American Physical Society

give the correct answer to a question posed to them in as many cases as possible under the constraint of restricted communication. Yet, one can imagine situations where not a single but two questions are posed to the parties and where the parties are restricted both in communication and in broadcasting of their answers. The specific case which is considered here is that the parties must give a *single* answer to *two* questions. Further, the parties are *not* allowed to differ in their answers. That is, they *must* produce two identical answers each time.

Formally the two questions will be formulated as a problem of computation of two three-valued functions f_1 and f_2. Since the parties are allowed to give only one answer about the values of two functions, their goal will be to give the correct value of f_1 with the *highest* possible probability, and at the same time, the correct value of f_2 with the *lowest* possible probability, while exchanging only a restricted (each party sending one trit) amount of information [16].

We now introduce the two-party task in detail and we give the functions f_1 and f_2 explicitly:

Alice receives a string $x = (x_0, x_1)$ and Bob a string $y = (y_0, y_1)$. Alice's string is a combination of a bit $x_0 \in \{0, 1\}$ and a trit $x_1 \in \{1, e^{i(2\pi/3)}, e^{-i(2\pi/3)}\}$. Similarly Bob's string is a combination of a bit $y_0 \in \{0, 1\}$ and a trit $y_1 \in \{1, e^{i(2\pi/3)}, e^{-i(2\pi/3)}\}$ (the representation in terms of complex third roots of unity is chosen for mathematical convenience). All possible input strings are distributed randomly and with equal probability.

Before they broadcast their answers, Alice and Bob are allowed to exchange two trits of information.

Alice and Bob each broadcast her/his answer in the form of one trit. The two answers must be identical. That is, they each broadcast the same one trit.

The task of Alice and Bob is to maximize the difference between the probabilities, $P(f_1)$, of giving the correct value for function

$$f_1 = x_1 y_1 e^{i(2\pi/3)(x_0 y_0)}, \tag{2}$$

and $P(f_2)$, of giving the correct value for function

$$f_2 = x_1 y_1 e^{i(2\pi/3)(2-x_0-y_0)}. \tag{3}$$

That is, they aim at the maximal value of

$$\Delta = P(f_1) - P(f_2). \tag{4}$$

We show that, if two parties use a broad class of classical protocols, the difference Δ of the probabilities for correct value of the two functions introduced above is at most 0.5, whereas if they use two entangled qutrits, this difference can be as large as $1/4 + 1/4\sqrt{11/3} \simeq 0.729$.

Note that the first factor $x_1 y_1$ in the full functions f_1 and f_2 results in completely random values if only one of the independent inputs x_1 or y_1 is random. This is not the case for the last factors with the inputs x_0 and y_0. Thus, *intuition* suggests that the optimal protocol for the two parties may be that Alice "spends" her trit in sending x_1 and Bob in sending y_1 and that they put for the second factor of the two functions a value which is most often appearing for function $e^{i(2\pi/3)(x_0 y_0)}$ (compare the third column in Table I) and, at the same time, least often appearing for function $e^{i(2\pi/3)(2-x_0-y_0)}$ (compare the fourth column). The second factor obtained in such a way is 1. Next, each of them broadcasts the value $x_1 y_1$ as her/his answer. In this way, $P(f_1) = 0.75$ and $P(f_2) = 0.25$, which gives $\Delta = 0.5$.

The second protocol suggested by intuition exploits the fact that f_2, in contradiction to f_1, is a factorizable function, i.e., $f_2 = (x_1 e^{i(2\pi/3)(1-x_0)})(y_1 e^{i(2\pi/3)(1-y_0)})$. Alice and Bob can exchange the values of $x_1 e^{i(2\pi/3)(1-x_0)}$ and $y_1 e^{i(2\pi/3)(1-y_0)}$. In this way, they both know the exact value of f_2. Thus, they broadcast a wrong value of it, e.g., $f_2 e^{-i(2\pi/3)}$. By looking at Table I, one immediately sees that this operation acts effectively as subtraction of 1 from the values in the last column. The obtained values agree with those in column three in two cases (two middle rows). Thus, within this protocol $P(f_1) = 0.5$ and $P(f_2) = 0$, which again results in $\Delta = 0.5$.

Let us now present a broad class of classical protocols which can be followed by Alice and Bob, and which contain the above intuitive examples as special cases:

Alice calculates locally any function $a(x_0, \lambda_A)$ and Bob calculates locally any function $b(y_0, \lambda_B)$ such that their outputs define the trit values to be broadcast under the restriction of communication. More precisely, Alice sends to Bob $e_A = a x_1$ and receives from him $e_B = b y_1$. Here λ_A and λ_B are any other parameters on which their functions a and b may depend. They may include random strings of numbers shared by Alice and Bob. Upon receipt of e_A and e_B, they both broadcast $e_A e_B$ as their answers (which always agree). Note that the first intuitive protocol is reproduced by $a = 1$ and $b = 1$ for all inputs. The second one is recovered by $a = e^{i(2\pi/3)(1-x_0)}$ and $b = e^{-i(2\pi/3)y_0}$ again for all inputs.

Before showing what is the maximal Δ achievable for such a wide class of classical protocols, we shall introduce its quantum competitor. Let Alice and Bob share a pair of entangled qutrits and suitable measuring devices (see, e.g., [17]). This is their quantum protocol:

If Alice receives $x_0 = 0$, she will measure her qutrit with the apparatus which is set to measure a three-valued

TABLE I. A set of possible input values for x_0 and y_0 and the corresponding values of the functions $x_0 y_0$ and $2 - x_0 - y_0$.

x_0	y_0	$x_0 y_0$	$2 - x_0 - y_0$
0	0	0	2
0	1	0	1
1	0	0	1
1	1	1	0

observable A_0 (Fig. 1). Otherwise, i.e., for $x_0 = 1$, she sets her device to measure a different three-valued observable A_1. Bob follows the same protocol. If he receives $y_0 = 1$, he measures the three-valued observable B_0 on his qutrit. For $y_0 = 0$ he measures a different three-value observable B_1. We ascribe to the outcomes of the measurements the three values 1, $e^{i(2\pi/3)}$, and $e^{-i(2\pi/3)}$ (the Bell numbers [17]). The actual value obtained by Alice in the given measurement will be denoted again by a, whereas the one of Bob's, also again, by b. Alice sends trit $e_A = y_1 a$ to Bob, and Bob sends trit $e_B = y_2 b$ to Alice. Upon reception of the transmitted values, they both broadcast $e_A e_B$ as their answers.

The task in both protocols is to maximize $\Delta = P(f_1) - P(f_2)$. The probability $P(f_1)$ is the probability for the product ab of the local measurement results to be equal to $e^{i(2\pi/3)(x_0 y_0)}$ in the two (classical and quantum) protocols:

$$P(f_1) = \tfrac{1}{4}[P_{A_0,B_1}(ab = 1) + P_{A_0,B_0}(ab = 1) + P_{A_1,B_1}(ab = 1) + P_{A_1,B_0}(ab = e^{i(2\pi/3)})], \quad (5)$$

where, e.g., $P_{A_0,B_1}(ab = 1)$ is the probability that $ab = 1$ if Alice measures A_0 and Bob measures B_1 (after she receives $x_0 = 0$ and he $y_0 = 0$). Recall that all four possible combinations for x_0 and y_0 occur with the same probability $\frac{1}{4}$. Similarly, the probability $P(f_2)$ that product ab is equal to $e^{i(2\pi/3)(2-x_0-y_0)}$ is given by

$$P(f_2) = \tfrac{1}{4}[P_{A_0,B_1}(ab = e^{-i(2\pi/3)}) + P_{A_0,B_0}(ab = e^{i(2\pi/3)}) + P_{A_1,B_1}(ab = e^{i(2\pi/3)}) + P_{A_1,B_0}(ab = 1)]. \quad (6)$$

Finally, one notices that the success measure in the task is given by

$$\Delta = \tfrac{1}{4} I_3, \quad (7)$$

where I_3 is exactly the Bell expression as defined by Collins *et al.* [12]. It is the combination of probabilities obtained here when the right-hand side of Eq. (5) is subtracted by the right-hand side of Eq. (6) and then multiplied by 4. Collins *et al.* [12] showed that $I_3 \leq 2$ for all local realistic theories. Recently the violation of this inequality was demonstrated for a pair of spin-1 entangled photons [18]. In Ref. [12] the local measurement results are defined differently (as numbers 0, 1, and 2); however, this description and the one used here are equivalent.

If one looks back at the family of classical protocols introduced above, one sees that they are equivalent to a local realistic model of the quantum protocol (λ's are local hidden variables, and x_1, y_1 are some local variables which are not hidden). This implies that within the full class of classical protocols considered here $\Delta \leq 0.5$.

Thus, the *necessary* and *sufficient* condition for the state of two qutrits to improve the success in our communication complexity task over any classical protocol of the discussed class is that the state violates the Bell inequality for two qutrits. Note that, except for shared entanglement, the discussed classical and quantum protocols are performed under the same conditions. A wider class of classical protocols could include local calculations of functions $a(x_0, x_1, \lambda_A)$, for Alice, and $b(y_0, y_1, \lambda_B)$, for Bob, which depend on the full local inputs. Note that then the quantum competitor could be based on Bell's experiment where the measurements can be chosen between six alternative three-valued observables. However, the fact that Δ in the intuitive classical protocols is equal to the maximal possible Δ in the discussed class of classical protocols strongly indicates that this class, although not the most general one, might already include the optimal one. This could be due to the different role of the entries x_0, y_0 and x_1, y_1 in the functions f_1 and f_2.

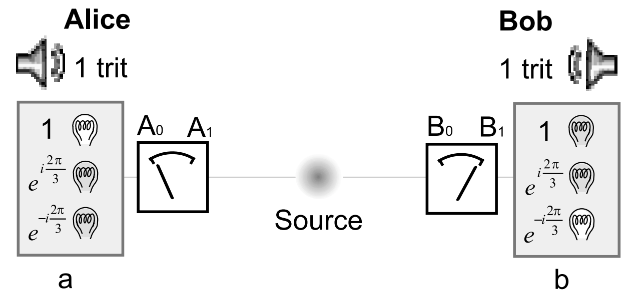

FIG. 1. Two-party quantum communication complexity protocol which is based on the Bell-type experiment with entangled qutrits. Alice receives a string $x = (x_0, x_1)$ and Bob $y = (y_0, y_1)$. Depending on the value of x_0 Alice chooses to measure between two different three-values observables A_0 and A_1. Similarly, depending on y_0 Bob chooses to measure between three-values observables B_0 and B_1. Alice's result of the measurement is denoted by a and Bob's by b. In the last step of the protocol, Alice sends the trit $x_1 a$ to Bob and Bob sends the trit $y_1 b$ to Alice.

It was shown in Ref. [19] that a nonmaximally (asymmetric) entangled state of two qutrits that reads: $|\psi\rangle = \frac{1}{\sqrt{2+\gamma^2}}(|00\rangle + \gamma|11\rangle + |22\rangle)$ with $\gamma = (\sqrt{11} - \sqrt{3})/2 \simeq 0.7923$ can violate the Collins *et al.* Bell inequality stronger than the maximally entangled one. In that case, the Bell expression I_3 reaches the value $1 + \sqrt{11/3} = 2.9149$. This implies that with the use of this particular state the probability difference Δ in our protocol can be as large as 0.729.

Therefore, in a classical protocol, even with shared random variables, more than two trits of information are *necessary* to complete the task successfully with Δ at least 0.729, whereas with the quantum entanglement two trits are *sufficient* for the task with the same Δ. Note that the discrepancy between the measure of success in the classical and the quantum protocol is higher here than in the two-party communication complexity problem of

Ref. [7] mentioned above. Here we have $\Delta_Q - \Delta_C \approx 0.23$, whereas there $P_Q - P_C \approx 0.1$.

As another example, we formulate a standard communication complexity task which is an immediate generalization of the one of Ref. [7]. In this case the task of Alice and Bob is only to maximize the probability for correct computation of function f_1. Since this is just a first part of the task introduced above, the highest possible probability of success in a classical protocol is $P_C = 0.75$. The connection with the violation of a Bell's inequality is established through equation $P_C = I_2/4$, where I_2 is another Bell expression [which is equal to Eq. (5) with the factor $\frac{1}{4}$ dropped] introduced in Ref. [12]. For all local realistic theories $I_2 \leq 3$. Therefore, all quantum states of entangled qutrits which violate this Bell inequality can lead to higher than classical success rate for the task.

We note that a series of similar specific two-party communication complexity tasks can be formulated with quantum solutions which exploit the possibility of two arbitrarily high-dimensional quantum systems to violate the corresponding Bell inequalities of Ref. [12].

As noted in Ref. [11], one may ask whether the use of qutrits is necessary for any quantum information task, because qutrits can be teleported with the help of singlets and classical communication. Yet any such realization would require more communication than permitted by our protocol. One may also ask whether the exclusive use of the states which violate Bell's inequalities is necessary for the problem, as there are nonseparable states which do not directly violate Bell's inequalities [20] but only after local operations and classical communication [21]. Yet again such transformation would require additional communication.

We interpret our work as a further example suggesting that the violation of Bell inequalities can be considered as a "witness of useful entanglement." This was first coined and suggested in [22,23] in different contexts.

M. Ż. acknowledges KBN Grant No. 5 P03B 088 20. Č. B. is supported by the Austrian FWF Project No. F1506 and by the European Commission, Contract No. ERBFMRXCT96-0087. This work is a part of the Austrian-Polish program "Quantum Communication and Quantum Information IV" (2002–2003).

[1] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, Cambridge, U.K., 2000).
[3] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC 1978)* (ACM Press, New York, 1979), pp. 209–213.
[4] G. Brassard, e-print quant-ph/0101005.
[5] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
[6] L. K. Grover, e-print quant-ph/9704012.
[7] H. Buhrman, R. Cleve, and W. van Dam, e-print quant-ph/9705033.
[8] H. Buhrman, W. van Dam, P. Hoyer, and A. Tapp, Phys. Rev. A **60**, 2737 (1999).
[9] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002); D. Bruß and C. Macchiavello, *ibid.* **88**, 127901 (2002).
[10] A. Ambainis, in *Proceedings of the 33rd Annual ACM Symposium on Theory of Computation (STOC 2001)* (ACM Press, New York, 2001), pp. 134–142.
[11] M. Fitzi, N. Gisin, and U. Maurer, Phys. Rev. Lett. **87**, 217901 (2001).
[12] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).
[13] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[14] E. F. Galvao, e-print quant-ph/0009014.
[15] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[16] In the case of three-valued functions, one can formulate two types of questions: (a) what is the actual value of a given function (in our example of f_1), or (b) what is an exemplary wrong value of a given function (in our example of f_2)? The answer to each question can be encoded in one trit. Note a fundamental difference with the case of two-valued functions. In the latter case, the wrong value uniquely defines the right one. This symmetry is broken for three-valued functions. A one-trit message revealing a wrong value does not reveal the right one. One may wonder whether tasks such as (b) ever appear in life. On many of the European TV networks, one can watch a quiz usually called "Millionaires." The player there should answer multiple-choice questions, but if he does not know an answer, then once in the game he is allowed to use a rescue measure. He can ask the computer to eliminate some, but not all, wrong answers. This is exactly a task such as the one for Alice and Bob here in the case of function f_2. Such a formulation of the task is in the spirit of the article by A. M. Steane and W. van Dam, Phys. Today, Feb. 2000, 35-39, who use the "guess my number game" to explain the task of Ref. [7].
[17] M. Żukowski, A. Zeilinger, and M. A. Horne, Phys. Rev. A **55**, 2564 (1997).
[18] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. (to be published).
[19] A. Acin, T. Durt, N. Gisin, and J. I. Latorre, e-print quant-ph/0111143.
[20] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[21] S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).
[22] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001).
[23] A. Acin and V. Scarani, e-print quant-ph/0112102; A. Acin, V. Scarani, and M. M. Wolf, e-print quant-ph/0206084.